HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200309084-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	David Andrew Thomas et al.	Confirmation No.:	3543
Application No.:	10/679,092	Examiner:	Benjamin E. Lanier
Filing Date:	October 3, 2003	Group Art Unit:	2132

Title: METHOD AND SYSTEM FOR CONTENT DOWNLOADS VIA AN INSECURE COMMUNICATIONS CHANNEL TO DEVICES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on September 4, 2008.

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

□ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $130 □ 2nd Month $490 □ 3rd Month $1110 □ 4th Month $1730

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

□ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: November 4, 2008

Typed Name: Judy H. Chung

Signature: Judy Chung

Respectfully submitted,

David Andrew Thomas et al.

By

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: November 4, 2008

Telephone: (703) 652-3822

Rev 10/08(AplBrief)

Total number of pages: 31

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200309084-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): David Andrew Thomas et al.

Confirmation No.: 3543

Application No.: 10/679,092

Examiner: Benjamin E. Lanier

Filing Date: October 3, 2003

Group Art Unit: 2132

Title: METHOD AND SYSTEM FOR CONTENT DOWNLOADS VIA AN INSECURE COMMUNICATIONS CHANNEL TO DEVICES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on September 4, 2008.

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

□ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $130 □ 2nd Month $490 □ 3rd Month $1110 □ 4th Month $1730

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

□ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: November 4, 2008

Typed Name: Judy H. Chung

Signature:

Respectfully submitted,

David Andrew Thomas et al.

By

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: November 4, 2008

Telephone: (703) 652-3822

Rev 10/05(AplBrief)

Total number of pages: 31

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 200309084-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): David Andrew Thomas et al.

Confirmation No.: 3543

Serial No.: 10/679,092

Examiner: Benjamin E. Lanier

Filed: October 3, 2003

Group Art Unit: 2132

Title: METHOD AND SYSTEM FOR CONTENT DOWNLOADS VIA AN INSECURE COMMUNICATIONS CHANNEL TO DEVICES

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action mailed June 6, 2008, and in connection with the Notice of Appeal filed September 4, 2008. It is respectfully submitted that the present application has been more than twice rejected. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

TABLE OF CONTENTS

(1) Real Party in Interest 3

(2) Related Appeals And Interferences 3

(3) Status of Claims 3

(4) Status of Amendments 3

(5) Summary of Claimed Subject Matter 3

(6) Grounds of Rejection to be Reviewed on Appeal 9

(7) Arguments 10

A. The objection to the specification should be reversed. 10

B. The rejection of claims 1-17, 21-23, and 27-29 over Wiser in view of Parenty under 35 U.S.C. §103(a) should be reversed. 10

C. The rejection of claims 20 and 26 over Wiser in view of Parenty in further view of Katayama under 35 U.S.C. §103(a) should be reversed. 14

(8) Conclusion 16

(9) Claim Appendix 17

(10) Evidence Appendix 28

(11) Related Proceedings Appendix 29

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1-30 are pending. Claims 18, 19, 24, 25 and 30 are withdrawn. Claims 1-17, 20-23, 26-29 are rejected, of which claims 1, 20-22, and 26-29 are independent. Claims 1-17, 20-23, 26-29 are all appealed.

(4) Status of Amendments

No amendment was filed subsequent to the Final Office Action dated June 6, 2008.

(5) Summary of Claimed Subject Matter

It should be understood that the subject matter of independent claims 1, 20-22, and 26-29 is supported in at least the following cited sections of the present application. Thus, other sections in the present application may provide the same or additional supports as well.

Claim 1. A method for facilitating content downloads via an insecure communications channel, comprising:

receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device; See page 9, line 10-page 11, line 21; Fig. 3.

transmitting encrypted content via the insecure communications channel from a content server to the device; See page 9, line 10-page 11, line 21; Fig. 3.

receiving the shared secret in plaintext form via a secure communications channel; See page 9, line 10-page 11, line 21; Fig. 3.

receiving a confirmation authorizing release of a decryption key; and See page 9, line 10-page 11, line 21; Fig. 3.

sending the decryption key for decryption of the encrypted content. See page 9, line 10-page 11, line 21; Fig. 3.

Claim 20. A method of authorizing a release of a decryption key corresponding to a downloaded content, comprising:

receiving from a user via a secure channel a shared secret in a plaintext form; See page 20, line 13-page 21, line 13; Fig. 6.

sending the shared secret to a content server; See page 20, line 13-page 21, line 13; Fig. 6.

receiving a confirmation of successful encrypted content download from the content server; See page 20, line 13-page 21, line 13; Fig. 6.

after receiving the confirmation of successful encrypted content download from the content server, prompting the user to accept terms of download and decryption of the encrypted content; and See page 20, line 13-page 21, line 13; Fig. 6.

after receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content. See page 20, line 13-page 21, line 13; Fig. 6.

Claim 21. A system for transmitting a file to a device, comprising:

a content server operative to store a plurality of content files, to wirelessly transmit the content files via an insecure channel, and to communicate with via a secure channel; See page 4, line 27-page 9, line 9; Figs. 1-2.

one or more remote devices operative to transmit and receive communications to and from the content server over the insecure channel including anyone of the content files in encrypted form, each device including a processor to manage the communications as well as encryption and decryption of communicated data; See page 4, line 27-page 9, line 9; Figs. 1-2.

a point of sale terminal operative to communicate with a user associated with any of the devices; and See page 4, line 27-page 9, line 9; Figs. 1-2.

a payment server communicatively disposed between the point of sale terminal and the content server, and communicating therewith via the secure channel, further operative to provide a shared secret in plaintext form via the secured channel from the user to the content server, wherein the content server is further operative to release a decryption key to one of the devices upon receipt of confirmation from payment server that the user of the device accepted terms of download and decryption of a content file, wherein the decryption key is encrypted using the shared secret. See page 4, line 27-page 9, line 9; Figs. 1-2.

Claim 22. A computer readable program embodied on a tangible computer readable medium for facilitating content download from a content server to a device via an insecure communications channel, comprising:

program code for causing a computer to receive a shared secret in an encoded form from a device, the encoded shared secret functioning as a device identifier; See page 15, line 10-page 20, line 12; Fig. 5.

program code for causing a computer to transmit content in an encrypted form from a content server to the device; See page 15, line 10-page 20, line 12; Fig. 5.

program code for causing a computer to receive the shared secret in plaintext form via a secure channel; See page 15, line 10-page 20, line 12; Fig. 5.

program code for causing a computer to receive a confirmation authorizing the release of a decryption key for the transmitted encrypted file; and See page 15, line 10-page 20, line 12; Fig. 5.

program code for causing a computer to send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received. See page 15, line 10-page 20, line 12; Fig. 5.

Claim 26. A computer readable program embodied on a tangible computer readable medium for authorizing a release of a decryption key corresponding to a downloaded content, comprising:

code for receiving a shared secret in a plaintext form from a user, via a secure channel; See page 20, line 13-page 21, line 13; Fig. 6.

code for sending the shared secret to a content server; See page 20, line 13-page 21, line 13; Fig. 6.

code for receiving a confirmation of successful encrypted content download from the file server; See page 20, line 13-page 21, line 13; Fig. 6.

code for prompting the user to purchase the downloaded encrypted content after receiving the confirmation of successful encrypted content download from the content server; and See page 20, line 13-page 21, line 13; Fig. 6.

code for, after receipt of payment, sending an authorization to the content server to release a decryption key operative to decrypt the downloaded encrypted file. See page 20, line 13-page 21, line 13; Fig. 6.

Claim 27. A method of facilitating content download via an insecure communications channel, comprising:

receiving a concealed identifier from a device wherein the concealed identifier identifies the device; See page 9, line 10-page 11, line 21; Fig. 3.

transmitting an encrypted file to the device via an insecure channel, wherein the encrypted file has a corresponding decryption key; See page 9, line 10-page 11, line 21; Fig. 3.

receiving the identifier in an unconcealed form over a secure channel; See page 9, line 10-

page 11, line 21; Fig. 3.

receiving an authorization from a payment server over the secure channel; See page 9, line 10-page 11, line 21; Fig. 3.

encrypting the key using the identifier; and See page 9, line 10-page 11, line 21; Fig. 3.

transmitting the encrypted key to the device. See page 9, line 10-page 11, line 21; Fig. 3.

Claim 28. A method for payment of file downloads to a wireless device, comprising:

receiving a concealed identifier from a device, wherein the identifier corresponds to the wireless device; See page 9, line 10-page 11, line 21; Fig. 3.

transferring a selected encrypted file to the wireless device, wherein the selected file is encrypted using a key; See page 9, line 10-page 11, line 21; Fig. 3.

receiving the identifier in an unconcealed form over a secure channel as part of a payment transaction; See page 9, line 10-page 11, line 21; Fig. 3.

using the identifier to encrypt the key; and See page 9, line 10-page 11, line 21; Fig. 3.

transmitting the encrypted key to the wireless device after receipt of payment. See page 9, line 10-page 11, line 21; Fig. 3.

29. A system for transmitting content via an insecure communications channel, comprising:

means for receiving a shared secret in an concealed form, from a device, wherein the shared secret identifies the device; See content server 6; page 9, line 10-page 11, line 21; Fig. 3.

means for transferring a selected content in an encrypted form to the device, wherein the selected file has a corresponding decryption key; See content server 6; page 9, line 10-page 11, line 21; Fig. 3.

means for receiving the shared secret in an unconcealed form over a secure channel as part of a payment transaction; See content server 6; page 9, line 10-page 11, line 21; Fig. 3.

means for using the shared secret to encrypt a decryption key; See content server 6; page 9, line 10-page 11, line 21; Fig. 3.

means for transmitting the encrypted decryption key to the wireless device after receipt of payment. See content server 6; page 9, line 10-page 11, line 21; Fig. 3.

(6) Grounds of Rejection to be Reviewed on Appeal

A. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter.

B. Claims 1-17, 21-23, and 27-29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Wiser (6,385,596) in view of Parenty (2002/0064283).

C. Claims 20 and 26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Wiser (6,385,596) in view of Parenty (2002/0064283), and further in view of Katayama (2002/0027994).

(7) Arguments

A. The objection to the specification should be reversed.

The specification was objected to because the phrase "tangible computer readable medium" allegedly lacks antecedent basis in the specification. This phrase is recited in claims 22 and 26.

"Computer readable medium" was recited in originally filed claims 22 and 26, and thus clearly there is support and antecedent basis for this phrase. The "tangible" computer readable medium includes, for example, any tangible computer readable medium which is inherently provided in the PDA's described on pages 4 and 5 of the specification. In particular, page 5, line 24 recites the PDA includes a memory and processing capabilities. One of ordinary skill in the art would readily recognize that a tangible computer readable medium in a PDA comprising programming code, as described in claim 22, includes any storage medium, such as the memory recited on page 5 of the specification. Accordingly, support is provided in the specification for "tangible computer readable medium," and the objection should be reversed.

B. The rejection of claims 1-17, 21-23, and 27-29 over Wiser in view of Parenty under 35 U.S.C. §103(a) should be reversed.

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex Inc.*, 550 U.S._, 82 USPQ2d 1385 (2007):

> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." Quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966).

According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

> (A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) "Obvious to try"—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S._, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Furthermore, as set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385.

If the above-identified criteria and rationales are not met, then the cited references fail to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited references.

Claim 1 recites,

> receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device; ...
> receiving the shared secret in plaintext form via a secure communications channel.

Wiser in view of Parenty fails to teach or suggest receiving a shared secret via an insecure channel. The rejection alleges this feature is disclosed by Wiser, because Wiser discloses a client transmits a credit card number using SSL v3. However, SSL is a secure channel and not an insecure channel. See Applicants' background, fourth paragraph. See also paragraphs 33 and 36 of Parenty.

The Final Office Action on page 3, paragraph 5, asserts that this argument is not persuasive because SSL is a protocol and not a channel. However, the Examiner fails to recognize that use of SSL with any channel on the Internet makes the channel secure, as described in the Applicants' background, and Parenty paragraphs 33 and 36.

Wiser in view of Parenty fails to teach or suggest receiving a shared secret twice, but in two forms, *i.e.*, an encoded form and a plaintext form. According to the rejection, the shared secret is received once in encrypted form by the media licensing center in Wiser. However, neither Wiser nor Parenty singly or in combination teach or suggest a media licensing center receiving the credit card information twice, but in two different forms. Furthermore, there would be no need for the media licensing center in Wiser to receive the credit card information twice, because once it is received, the transaction can be completed.

Independent claim 21 recites, "wherein the decryption key is encrypted using the shared secret." The rejection alleges the credit card information of Wiser is the shared secret. However, Wiser in view of Parenty fails to teach or suggest a decryption key is encrypted with credit card information.

Independent claim 22 recites receiving a shared secret twice, but in two forms, *i.e.*, an encoded form and a plaintext form, similar to claim 1 described above. For the reasons described above with respect to claim 1, Wiser in view of Parenty fails to teach or suggest these features.

Independent claim 27 recites,

> receiving a concealed identifier from a device wherein the concealed identifier identifies the device; ...
> receiving the identifier in an unconcealed form over a secure channel; ...
> encrypting the key using the identifier.

Wiser in view of Parenty fails to teach or suggest receiving an identifier twice, once in a concealed form and once in an unconcealed form. Also, Wiser in view of Parenty fails to teach or suggest encrypting the key using the identifier. As described above, the rejection interprets the credit card information of Wiser as the claimed identifier. There is no disclosure in Wiser in view of Parenty of encrypting a key using credit card information.

Independent claims 28 and 29 recite features similar to the features of claim 27 described above. Accordingly, Wiser in view of Parenty fails to teach or suggest all the features of claims 28 and 29.

For at least these reasons, the rejection of claims 1-17, 21-23, and 27-29 over Wiser in view of Parenty should be reversed and these claims allowed.

C. The rejection of claims 20 and 26 over Wiser in view of Parenty in further view of Katayama under 35 U.S.C. §103(a) should be reversed.

Independent claim 20 recites,

> after receiving the confirmation of successful encrypted content download from the content server, prompting the user to accept terms of download and decryption of the encrypted content.

Independent claim 26 recites similar features.

The Final Office Action correctly admits Wiser in view of Parenty fails to teach or suggest that a content key is sent to a user after the encrypted content has been downloaded and in response to acceptance of terms. The Final Office Action, however, asserts Katayama, in paragraphs 64 and 78, discloses that a content key is sent to the user after the encrypted content is downloaded and in response to the purchase order for the content key.

In paragraphs 47 and 48, Katayama discloses that audio data is sent to the audio player 111 from the distribution device via a network. In paragraph 61, Katayama discloses that the audio data can be played in a degraded quality. In order to play the audio data in high quality, the audio player 111 needs a second key. The consumer can buy the second key after the initial receipt of the audio data in order to playback the audio in high quality. See Katayama, paragraphs 63 and 64.

Wiser discloses in column 8, lines 19-32 that a media voucher, including indication of a purchase of a media data file, is provided prior to sending the media file to the media player 116 of the user. Thus, Wiser discloses purchase is performed prior to the downloading of the media file to the media player. It would not have been obvious to combine the purchase of the second key of Katayama with Wiser, because in Wiser, the media file is already purchased prior to sending the media file. Thus, there would be no reason to purchase the media file again in Wiser. Hence, it would not have been obvious to one of ordinary skill in the art to combine Katayama with Wiser in view of Parenty, and the rejection of claims 20 and 26 should be reversed.

(8) Conclusion

For at least the reasons given above, the rejection of claims 1-17, 20-23, 26-29 described above and the objection to the Abstract described above should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: November 4, 2008

By

Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 652-3822
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. (Original) A method for facilitating content downloads via an insecure communications channel, comprising:

receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device;

transmitting encrypted content via the insecure communications channel from a content server to the device;

receiving the shared secret in plaintext form via a secure communications channel;

receiving a confirmation authorizing release of a decryption key; and

sending the decryption key for decryption of the encrypted content.

2. (Original) A method as recited in claim 1, wherein the confirmation is based on payment for the transmitted encrypted content.

3. (Original) A method as recited in claim 1, wherein the shared secret identifies a user, the device, or both.

4. (Original) A method as recited in claim 1, wherein the shared secret is a credit card number or a phone number.

5. (Original) A method as recited in claim 1, further comprising:

receiving from the device an acknowledgement indicating receipt of the decryption key.

6. (Original) A method as recited in claim 1, wherein the decryption key is sent to the device via the insecure communication channel.

7. (Original) A method as recited in claim 1, wherein the decryption key is sent in plaintext form to a point of sale terminal via the secure channel.

8. (Original) A method as recited in claim 1, further comprising:

receiving a random plaintext from the device.

9. (Original) A method as recited in claim 8, wherein the shared secret is encoded by a hash function of a combination of the shared secret and the random plaintext.

10. (Original) A method as recited in claim 8, further comprising:

encrypting the decryption key before sending it to the device.

11. (Original) A method as recited in claim 10, wherein the decryption key is encrypted using at least the shared secret and, optionally, the random plaintext secret.

12. (Original) A method as recited in claim 1, further comprising:

receiving from the device a content download confirmation value that is encoded with the shared secret.

13. (Original) A method as recited in claim 12, wherein the content download confirmation value is based on an MD5 checksum.

14. (Original) A method as recited in claim 12, wherein the content download confirmation value is based on a calculation using the shared secret.

15. (Original) A method as recited in claim 12, wherein the step of receiving confirmation further comprises:

receiving a random plaintext from the device;

receiving a hash of the shared secret and the random plaintext for each shared secret;

computing a hash of the shared secret with the random plaintext to produce a cyphertext for each shared secret;

comparing the cyphertext to each of the received hash of each of the shared secrets; and in the case of a match,

identifying the corresponding transmitted encoded content,

encoding a content download confirmation value for the transmitted encoded content using the shared secret; and comparing the computed content download confirmation value to the received content download confirmation value to verify a complete content download.

16. (Original) A method as recited in claim 15, further comprising:

after verification of the complete content download, causing a prompt to be sent to a user of the device to purchase the downloaded content; and

receiving a confirmation of receipt of payment.

17. (Original) A method as recited in claim 1, wherein content stored in the content server is encrypted prior to a start of a download process.

18. (Withdrawn) A method for downloading content from a content server over an insecure communications channel, comprising:

sending a shared secret in an encoded form to a content server via an insecure communications channel;

downloading from the content server an encrypted content via the insecure channel;

sending an encoded content download confirmation value to the content server via the insecure communications channel;

receiving a decryption key in an encrypted form from the content server via the insecure communications channel, wherein the decryption key is encrypted using the shared secret;

decrypting the downloaded decryption key using the shared secret;

decrypting the downloaded encrypted content using the decryption key; and

sending an acknowledgement of the received decryption key.

19. (Withdrawn) The method of claim 18 further comprising:

providing an indicia of acceptance of terms of the download and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

20. (Previously Presented) A method of authorizing a release of a decryption key corresponding to a downloaded content, comprising:

receiving from a user via a secure channel a shared secret in a plaintext form;

sending the shared secret to a content server;

receiving a confirmation of successful encrypted content download from the content server;

after receiving the confirmation of successful encrypted content download from the content server, prompting the user to accept terms of download and decryption of the encrypted content; and

after receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content.

21. (Original) A system for transmitting a file to a device, comprising:

a content server operative to store a plurality of content files, to wirelessly transmit the content files via an insecure channel, and to communicate with via a secure channel;

one or more remote devices operative to transmit and receive communications to and from the content server over the insecure channel including anyone of the content files in encrypted form, each device including a processor to manage the communications as well as encryption and decryption of communicated data;

a point of sale terminal operative to communicate with a user associated with any of the devices; and

a payment server communicatively disposed between the point of sale terminal and the content server, and communicating therewith via the secure channel, further operative to provide a shared secret in plaintext form via the secured channel from the user to the content server, wherein the content server is further operative to release a decryption key to one of the devices upon receipt of confirmation from payment server that the user of the device accepted terms of download and decryption of a content file, wherein the decryption key is encrypted using the shared secret.

22. (Previously Presented) A computer readable program embodied on a tangible computer readable medium for facilitating content download from a content server to a device via an insecure communications channel, comprising:

program code for causing a computer to receive a shared secret in an encoded form from a device, the encoded shared secret functioning as a device identifier;

program code for causing a computer to transmit content in an encrypted form from a content server to the device;

program code for causing a computer to receive the shared secret in plaintext form via a secure channel;

program code for causing a computer to receive a confirmation authorizing the release of a decryption key for the transmitted encrypted file; and

program code for causing a computer to send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received.

23. (Original) The computer program embodied on a computer readable medium of claim 22 wherein the confirmation is sent upon payment by a user of the device for the downloaded content.

24. (Previously Presented) A computer readable program embodied on a tangible computer readable medium for downloading content from a content server, over an insecure communications channel, comprising:

code for sending a shared secret in an encoded form to a content server;

code for receiving from the content server an encrypted content;

code for sending an encoded content download confirmation value to the content server;

code for receiving an encrypted decryption key from the content server, wherein the decryption key is encrypted using the shared secret;

code for decrypting the encrypted decryption key using the shared secret;

code for decrypting the downloaded encrypted content using the decryption key; and

code for sending an acknowledgement of the received decryption key.

25. (Withdrawn) The computer readable program embodied on a computer readable medium of claim 24 further comprising:

code for providing an indicia of acceptance of terms of the download and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

26. (Previously Presented) A computer readable program embodied on a tangible computer readable medium for authorizing a release of a decryption key corresponding to a downloaded content, comprising:

code for receiving a shared secret in a plaintext form from a user, via a secure channel;

code for sending the shared secret to a content server;

code for receiving a confirmation of successful encrypted content download from the file server;

code for prompting the user to purchase the downloaded encrypted content after receiving the confirmation of successful encrypted content download from the content server;

and

code for, after receipt of payment, sending an authorization to the content server to release a decryption key operative to decrypt the downloaded encrypted file.

27. (Original) A method of facilitating content download via an insecure communications channel, comprising:

receiving a concealed identifier from a device wherein the concealed identifier identifies the device;

transmitting an encrypted file to the device via an insecure channel, wherein the encrypted file has a corresponding decryption key;

receiving the identifier in an unconcealed form over a secure channel;

receiving an authorization from a payment server over the secure channel;

encrypting the key using the identifier; and

transmitting the encrypted key to the device.

28. (Original) A method for payment of file downloads to a wireless device, comprising:

receiving a concealed identifier from a device, wherein the identifier corresponds to the wireless device;

transferring a selected encrypted file to the wireless device, wherein the selected file is encrypted using a key;

receiving the identifier in an unconcealed form over a secure channel as part of a payment transaction;

using the identifier to encrypt the key; and

transmitting the encrypted key to the wireless device after receipt of payment.

29. (Original) A system for transmitting content via an insecure communications channel, comprising:

means for receiving a shared secret in an concealed form, from a device, wherein the shared secret identifies the device;

means for transferring a selected content in an encrypted form to the device, wherein the selected file has a corresponding decryption key;

means for receiving the shared secret in an unconcealed form over a secure channel as part of a payment transaction;

means for using the shared secret to encrypt a decryption key;

means for transmitting the encrypted decryption key to the wireless device after receipt of payment.

30. (Withdrawn) An apparatus for content download to a device via an insecure channel comprising:

means for receiving at least one identifier from a device, wherein the identifier is concealed and identifies the device;

means for transmitting an encrypted file to the device;

means for transmitting after receipt of an authorization, a decryption key encrypted using the identifier, wherein the decryption key can decrypt the encrypted file.

(10) Evidence Appendix

(11) Related Proceedings Appendix

None.